(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 April 2001 (19.04.2001)

PCT

(10) International Publication Number
WO 01/28154 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/FI00/00896

(22) International Filing Date: 13 October 2000 (13.10.2000)

(25) Filing Language: Finnish

(26) Publication Language: English

(30) Priority Data:
19992204 13 October 1999 (13.10.1999) FI

(71) Applicant *(for all designated States except US)*: HELSINGIN PUHELIN OYJ [FI/FI]; P.O. Box 148, FIN-00131 Helsinki (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: SALSTE, Tuomas [FI/FI]; Mäkitorpantie 29-31 A 12, FIN-00640 Helsinki (FI).

(74) Agent: BERGGREN OY AB; P.O. Box 16, FIN-00101 Helsinki (FI).

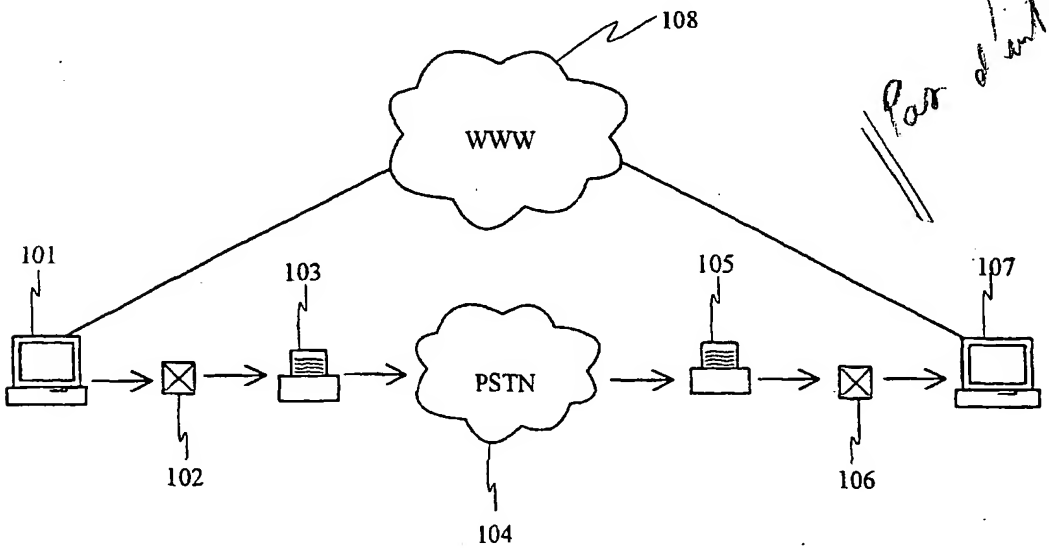
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

[Continued on next page]

(54) Title: TRANSMISSION OF CONFIDENTIAL INFORMATION



(57) Abstract: This invention concerns a method and a system for transmitting confidential information. The method according to the invention is particularly advantageously applied in a situation in which a part of the information to be transmitted can be transmitted via an open telecommunication network and another part is transmitted via a closed telecommunication network. According to the invention, the information that is transmitted via the closed telecommunication network is confidential information, such as a credit card number. In the method according to the invention, the data to be transmitted via the closed telecommunication network is preferably also encoded to improve data security. The system according to the invention comprises first means for transmitting information at least partly via an open telecommunication network, second means for encoding confidential information and third means for transmitting confidential information via a closed telecommunication network.

WO 01/28154 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Transmission of confidential information

This invention relates to a method and a system for transmission of confidential information. Particularly the invention concerns the transmission of this information in various telecommunication networks.

Today, when it is important to guarantee data security in the transmission of confidential information, the traditional manual data transfer methods are used. These include, for instance, communication by telephone or post. However, the importance of data networks is increasing and more and more information is transferred in open data networks. Here an open data network means a network used for data transfer, which is in public use and to which anyone can be connected when he so wishes. A typical open data network is the Internet, for example.

There has been a lot of discussion about the data security of open data networks. Especially the transmission of confidential information via open networks, such as the Internet, is very risky, because data security in open data networks is practically nonexistent. The data being transmitted there can be rather easily be analyzed by anyone.

Confidential information is most often transferred in facilities related to electric trade. In international electric trade, for instance, information related to credit cards is very important. When paying for purchases made electrically, the customer transmits to the seller the credit card number, the validity of the credit card and his personal data via e-mail, a www browser, telephone or telefax. The data security of the two first mentioned is much worse than that of the two last. In the worst case, a third party might obtain the credit card information transmitted through the data network and use it illegally for his own purposes.

In an open data network, a data security risk may arise for at least three different reasons. For example, when information is transferred via e-mail, it is not possible for the receiver to make sure who has sent the message. The sender of the message may request confidential information in the e-mail message, and the receiver may easily give the information without noticing that the sender is not entitled to receive the information. In the worst case, the receiver does not even know who is requesting the confidential information. Neither is any proof left to the receiver about the person who asked for the confidential information, if the e-mail message is removed.

Another problem is a potential third party intercepting between the sender and the receiver. The third party can copy the transmitted information for himself, but the original sender or the receiver of the message does not notice any problems in transmission. The copier of the messages will know the contents of the messages and can utilize the information. It is also possible that the third party "captures" the message, changes the contents and forwards the message to the receiver.

The third obvious problem, which is related to the previous, is the fact that the sender cannot be sure who the ultimate receiver of the message is. The message may go to a different receiver than was intended by the sender.

There have been attempts to improve the security of open data networks by various encrypting programs, by which files and the like can be encrypted so that an unauthorized third party gets no advantage of information received illegally. The encryption programs are based on mathematical algorithms, and solving them without certain information about the algorithm has been made as difficult as possible. However, no perfectly secure encrypting algorithm exists. Thus the effect of the algorithms is based on the fact that it takes so long to decrypt the algorithm that the encrypted information is outdated when it has been decrypted.

There are also problems in the use of the aforementioned encrypting algorithms. Firstly, programs in which the encrypting algorithms are used, are not used very commonly. In addition, the use of certain encrypting programs is even forbidden by national laws. The availability of some encrypting programs is restricted by various export limitations, which, among other things, prevent the sale from the country of programs offering too high encryption. The use of programs with too high encryption is forbidden by law in some countries, to allow the authorities of those countries to control the information moving in data networks when required, for the sake of national security, for example.

The specification EP 0 889 620 A2 discloses a method and a system, in which two different routes are used for data transfer. Information, which is not confidential, is transmitted via an open data network, such as the Internet. A closed network, which may be a telephone network, for example, is used for transmitting confidential information.

It is an objective of this invention to provide a method and a system, by which especially confidential information can be transmitted from the sender to the receiver so that no unauthorized third party has access to the information.

The objectives of the invention are achieved by an arrangement, by which confidential information is encoded and transmitted via a closed telecommunication network from the sender to the receiver. A special method, which can be tailored separately for each data transmission situation, is used for handling confidential information.

The method according to the invention is characterized in what is set forth in the characterizing part of the independent claim concerning the method.

The system according to the invention is characterized in what is set forth in the characterizing part of the independent claim concerning the system.

Preferred embodiments of the invention are set forth in the dependent claims.

In an arrangement according to the invention, the sender transmits the confidential information to the receiver via the closed telecommunication network. An example of such a closed telecommunication network is the public switched telephone network. The transmission of confidential information takes place so that the sender encodes the confidential information by a method agreed on between the sender and receiver. This method is preferably one that the receiver has provided for the use of the sender either for this data transfer event or for an earlier, corresponding data transfer event.

After the encoding, the sender transmits the coded data to the receiver over the closed telecommunication network by means of a telefax, for example. When the receiver has received the encoded data, he can use various methods for decoding it. In view of the efficiency of the system, the best are mechanical, automated decoding methods.

According to the invention, all the data, which does not contain confidential information, is transmitted via the open data network.

In the following, the invention will be described in more detail with reference to the accompanying drawings, in which

Fig. 1 illustrates the principle of the first system according to the invention,

Fig. 2 shows a flow chart of a method according to the invention,

Fig. 3 shows the signals of a system according to one embodiment of the invention,

Fig. 4 shows the signals of a system according to another embodiment of the invention, and

Fig. 5 illustrates the principle of another system according to the invention.

The same reference numbers and markings are used for similar entities in the figures.

A central idea of the invention is to use a closed telecommunication network, such as a public switched telephone network, for transmitting confidential information. A system like this provides many advantages. Firstly, because confidential information is not transmitted in the open data network, the risk of an unauthorized third party gaining access to the confidential information can be reduced. Because the confidential information is transmitted by a telefax, for example, via the public switched telephone network, it is possible when desired and required to send to the receiver a document with the sender's signature as an official indication of acceptance. Similarly, the sender thus has a receipt on paper of the information transmitted. Typically, the operator of the telephone network has information of the owners of each terminal. Thus the person sending confidential information can verify the telefax number of the receiver and thus make sure that the information to be transmitted goes to the right receiver. Especially in electric trade, the idea according to the invention is very useful, because credit card companies regard the telephone network as a safe way of transmitting confidential information and accept orders transmitted via a telephone network, unlike orders transmitted via open data networks.

The system shown in Fig. 1, by means of which the advantages of the invention are achieved, will now be described in more detail. Let us assume a situation in which a sender 101 is about to transmit confidential information to a receiver 107. The sender 101 has entered the confidential information into a computer and encodes it by means of a separate encoding device or program 102, for example. Such an encoder may be e.g. a bar code encoder or the like, and in practice it may be either a

completely separate device, an encoding card or circuit installed in the computer or an arrangement implemented entirely by means of software, or some combination thereof, by which the confidential information can be encoded. In the next step, according to this exemplary embodiment, the sender prints the encoded confidential information, inputs it to a telefax device and sends to the receiver. The confidential information is transmitted via a Public Switched Telephone Network (PSTN) to the receiver. According to a preferred embodiment, at the receiving end the telefax device prints the received data, which is inputted to a decoder 106, which decodes the information that was encoded at the transmitting end. The decoding device 106 is inverse to the encoding device 102, and it may similarly be implemented either as a completely separate device, a decoding card or circuit installed in the computer or an arrangement implemented entirely by means of software in the computer, or a combination thereof. The decoded, plain data is inputted to the receiver's computer 107, for example, by means of which the receiver can read the message received.

Telecommunications between two computers can be handled via an open data network, such as the Internet (WWW; World Wide Web) 108, when the data to be transmitted does not contain confidential information. The solution according to the invention provides the advantage that confidential information can be transmitted as almost completely protected from the sender to the receiver. The above mentioned public switched telephone network can be understood more widely as a network in which data security is better than in an open data network. One such network is the mobile communication network, for example. In the exemplary embodiment of the invention presented here, the use of separate encoding in the transmission of confidential information has been mentioned, but it is clear that encoding can also be left out when desired. When desired, encoding can also be used in connection with the information, which is transmitted via an open data network. For the invention it is essential that the system according to the invention comprises at least first means by which at least part of the information to be transmitted can be transmitted via an open data network and second means by which at least confidential information can be transmitted via a closed telecommunication network. In addition, a system according to the invention can comprise means for encoding and/or decoding the information to be transmitted. The means can be, for example, such that the information can be encoded as bar codes.

Fig. 2 shows a flow chart of the method according to the invention in a simple manner. According to the invention, in the first step 201 the sender gives the information, after which a decision is taken 202 as to whether the information given

contains such information to which access should not be allowed for third parties. If the information does not contain confidential information, the information is transmitted from the sender to the receiver in an open data network 203. If again the information contains confidential information, the information is transmitted in a closed telecommunication network 204, such as a public switched telephone network.

Let us then discuss the application of an arrangement according to the invention for a special use, such as electric trade via the Internet, which is shown in Fig. 3. In the first step, the buyer is in the home page of the service provider and, for example, selects the desired products by using a known method. Making a selection means that the buyer sends in step 301 the selected information, or information telling what he wants to buy, to the receiver or seller via an open data network. At this stage, no confidential information is transmitted between the sender and receiver, although in order to protect the privacy of the buyer it may sometimes be important that no outsiders will know who wants to buy what from whom. In order to encrypt this information, which has a low level of confidentiality but is nevertheless not public, it is possible to use in step 301 any method which is intended for use in an open data network and is known as such, but this is of no consequence with regard to the invention.

When the system of the seller has received the order information, it transmits in step 302 either automatically or as guided by the user a reply to the seller, in which reply it asks for the credit card information from the buyer, for example. Other information that can be requested include the personal data and address data, by means of which the seller can deliver the selected products to the buyer. According to an especially advantageous embodiment of the invention, in connection with the reply, the seller's system also transmits to the buyer a separate encoding program, by means of which the buyer can encode the required confidential information to improve the protection. Some possibilities for implementing such an encoding program in practice will be described in more detail in the following.

According to the embodiment shown in Fig. 3, the purpose of the encoding program is both to offer the buyers an easy possibility of inputting confidential information to the terminal at their disposal and to make confidential transmission of this information to the receiver as easy and reliable as possible. For inputting the information, the encoding program includes a so-called form, which is a file or a part of a file, which can be presented to the buyer via the user interface of the

terminal at his disposal. Typically the form is a file or a part of a file, which can be presented to the buyer graphically in the display of a computer or a corresponding terminal. The form contains fields in which the buyer should enter certain data, at least part of which are confidential. In addition, the form preferably includes instructions for filling in the fields. When the encoding program is delivered to the buyer, all the fields of the form may be empty or there may be some prefilled data in some of them. The prefilled data used by the seller's system can be either purely exemplary, in which case they have nothing to do with the buyer in question, or they can be data, which the seller's system has collected of the buyer in question either during the buyer's establishment of a connection in step 301 or earlier when the same buyer has had a connection with the seller's system.

The encoding program also includes some kind of a filling-in function, by means of which the buyer can fill in the data wanted in the form. In simple user interfaces equipped with a keyboard, display and possibly a mouse, a function like this includes means for moving a cursor to a certain field as a response to a control command given by the user and means for saving a certain piece of input data when the user has moved the cursor to a certain field and keys in a certain character string. The implementation of the form and the filling-in function represent a technology well known as such in the art.

As its name implies, the encoding program includes an encoding function. In this connection, the term encoding is used for any operation in which the input data given by the user are converted into a form in which they can be delivered to the seller via a closed telecommunication network and in which they can be later read by the seller or the system at the seller's disposal. One well-known encoding method is converting character strings into a bar code, which is printed on paper or saved in a form, which corresponds to the optically read bar code. Here the term bar code means a sequence formed by consecutive areas with a simple shape and different optical reflectivity. The bar code can be one-dimensional, in which case it can be read simply by reading the optical reflectivity profile along an imaginary line running over the bar code, or it may be two-dimensional, in which case it can also be called square code. Another well-known encoding method is printing character strings on paper with marks that are intended to be read optically. An example of the latter marks are alphanumeric marks that are used in cheques and other paper documents used in the banking business. Encoding may also include a function in which a piece of input data given in a human-readable form (such as a plain credit card number) is converted into a form in which it is not readable by humans.

However, such a coding function, which reduces readability, is not necessary with regard to the invention. At the simplest, encoding may be a null operation, which means saving the character strings entered by the buyer as such.

In addition, the encoding program includes a printing function, which may be an independent part of the encoding program or part of the encoding described above. Printing as such means in this connection final conversion of the encoded input information into a form in which they can be left to be transmitted by the closed telecommunication network. If it is assumed that a system according to Fig. 1 is used, printing means concrete printing of the encoded input information on paper, which can be fed to a telefax device used by the buyer. Producing a paper print can also be avoided so that the encoded input data are directly converted electrically to the form into which the transmitting telefax device would in any case convert them when optically reading the paper fed into it. This requires that the printing function of the encoding program is of the type of a programmed fax modem, which can "print" the electric data in computer-readable form into a bitmap used by the telefax devices in their mutual data transfer. Implementing such a function may require that the buyer's computer has a modem either as a separate device or in the form of a modem card installed in the computer. If the public switched telephone network is used as the closed telecommunication network without telefax devices, the printing function must be one that converts the encoded input data into tone frequency signals. Many alternative printing forms and means for using them in connection with the invention essentially in the above described manner are known from the prior art. Certain technical limitations must be taken into account in the selection of the printing method: if paper prints are used, the printing area must be such that it fits the printing papers most commonly used in the world (cf. the differences between the European A4 size and the Anglo-Saxon letter size). In addition, the characters to be printed must be large enough so that copying them would not reduce their readability. The fonts must be as widely used as possible and such that a slight deterioration in the printing quality would not make the letters disturbingly similar to each other.

In order to improve security, the encoding program may also include an encrypting function. Encryption means all such operations the purpose of which is to convert the input data given by the buyer into a form in which it is possible to read and to interpret them correctly only when using the right decrypting key. In the prior art, there is known a so-called public and private key method, in which the keys form unambiguous pairs. Information that has been encrypted by a certain so-called

public key can only be opened with a corresponding private key. It is impossible to determine the shape of the other half of the pair of keys only on the basis of the other half. The encoding program may contain the public key of the seller and means for encrypting the information given by the buyer with this key before encoding it or at the latest before printing it. The use of encryption improves data security, because it protects the parties of the connection against tapping of the telephone network, wrongly dialled telephone numbers or the possibility that a transmitted or received telefax message remains lying on the telefax device, where it can be read by a large number of people, for example.

Furthermore, the encoding program may include a function to identify the buyer, the purpose of which is that only the buyer who at the time wants to do business with the seller can transmit the information formed by the encoding program through the closed data network. A simple method of identifying the buyer is based on the fact that the buyer has either earlier in step 301 delivered his public encryption key to the seller or placed one in a public database for the use of the seller. When sending the encoding program to the buyer, the seller encrypts it with the buyer's public key. Only the intended buyer can utilize such an encoding program transmitted as encrypted, because only he has the private key by which the encryption can be opened.

In addition, the encoding program may include an electric signing function. In the embodiment of the invention shown by Fig. 1, in which the buyer prints the information produced by the encoding program on paper before sending it by telefax, signing can also be done traditionally with a pen: the buyer writes his signature on the printed paper before inputting it to the telefax. Electric signing means that the input data are encrypted with the buyer's private key at some stage before sending them to the seller. Information that has been so encrypted can only be opened with the buyer's public key, which must be verified: a so-called independent party has verified that a certain public key belongs to a certain buyer. An electric signature is easier to use than the traditional method, because an electric signature can also be verified electrically, unlike the traditional signature based on handwriting and its special physical characteristics.

The encoding program can also include a transmission function, by means of which the confidential information is transmitted via the closed data transfer network to the seller. A transmission program is not needed in the embodiment of Fig. 1, for example, because the transmission is handled by a program which controls the

operation of the buyer's telefax device. On the other hand, if the printing operation is handled by a program of the type of a telefax or tone frequency modem and a modem in the buyer's computer, the transmission function is naturally combined with printing, because in addition to the actual processing, the modems can also handle the setup and use of a telecommunication connection so that the data can be transmitted to the seller via a closed telecommunication network.

The form in which the encoding program is delivered to the buyer in step 302, depends somewhat on the equipment used by the buyer and seller for communication according to Fig. 3. It has been assumed above that the buyer's terminal is a computer. Then the encoding program can have the form of a Java program, i.e. an applet, a JavaScript or VBScript program, i.e. a script, a browser or a part thereof, i.e. a plug-in or executable binary program or an exe file. If the user's terminal is a mobile station, for example, the form of the encoding program must be such that the operating system of the mobile station or a program running under it and controlling the operation of the mobile station can recognize the encoding program as an executable program and install it to executable readiness. The buyer's original connection setup in step 301 may contain information about the type of the buyer's terminal or some other information as to what kind of an encoding program the buyer's terminal can utilize. It is common knowledge to a person skilled in the art how to write encoding programs which can be utilized by buyers' different terminals.

In step 303, the encoding program is installed and started automatically to executable readiness or the buyer starts it with a separate command given to the terminal. The program can also be installed automatically but require a command to be started. In addition, in step 303 the buyer inputs the information requested by the encoding program, and the encoding program encodes it.

The fact that the encoding program is a program intended to be executed by a computer or the like constitutes a certain risk for the buyer. The buyer should be able to make sure that no virus is installed to his terminal with the encoding program. The virus risk can be prevented by using authentication of the seller and controlling the integrity of the encoding program, of which the previous means the use of cryptographic means known as such to make sure that the party acting as the seller is what the buyer thinks it is. The control of the integrity of the encoding program means using cryptographic means known as such to make sure that the

contents of the executable program acting as an encoding program have not changed after the seller has produced it for transmission to the buyer(s).

Internet browsers, which represent the prior art at the priority day of this patent application, have security properties which can, for example, prevent writing any kind of information received via the network on the fixed disk of the buyer's terminal. Such a data security property does not impede the use of an encoding program described above, because the encoding program can be executed without needing to write anything on the hard disk. This is the case especially if the coding program is in the form of a script. After the execution or in connection with the next shutting down of the computer or other operation which means emptying the run-time memory of the computer, such a program which is executed without saving disappears from the memory of the terminal. Thus the confidential information received by it from the buyer are not saved in the buyer's computer, either.

Step 304 means printing in the sense described above. According to a first embodiment of the invention, the buyer prints the information on paper, signs the information by pen or stamp and transmits the information by telefax or a corresponding device, which converts graphical information into electric form via the public switched telephone network to the seller. The transmission has been denoted with the reference number 305. According to another preferred embodiment, the buyer forwards the confidential information, which may be encoded, to be transmitted electrically by telefax. Such an arrangement requires of the buyer's system that the computer or computer network and the telefax device are connected to each other, but such connecting is a technique known as such. According to a third embodiment, the buyer also signs the confidential information electrically, e.g. by means of a system in which a public key and a private key are used to implement the signature. In the near future, in accordance with a preferred embodiment of the invention, the information of an electric identification card can be used instead of the signature. Naturally this requires that the buyer has at his disposal means for reading and transmitting the information of the chip of the identification card.

The seller receives the confidential information by means of a device in his own use, which can communicate via a closed telecommunication network. The use of a telefax has been frequently mentioned above, and thus it can again be assumed as an example that the seller receives confidential information by a separate telefax device or a telefax modem operating as a part of the computer system. Even if the seller's

telefax device is physically separate and not directly a part of a computer or a computer system, it can have a local data transfer connection to a data system of the seller, which comprises means for reading, decoding and saving information received from the buyers. In order to make the operation faster, it is advantageous that the seller's data system can automatically combine the received confidential information to purchase information transmitted earlier in step 301. The combining can take place on the basis of the transmitting telefax number or the like, which has been given to the seller already when purchases have been made via the Internet. In Fig. 3, the transmission of confidential information of the buyer 305 is marked with a broken line, which means that this transmission of information takes place via a closed telecommunication network.

In the embodiment according to Fig. 3, the seller sends in step 306 to the buyer verification of successful reception of confidential information. Such a so-called acknowledgement is preferably arranged to take place automatically as a consequence of the operation of the seller's data system. The acknowledgement 306 is marked in the figure with a solid line to indicate that an open telecommunication network can be used as a transmission channel for it. Alternatively it can be sent in the closed telecommunication network; the channel in which the acknowledgement is sent is of no consequence with regard to the invention. Neither is the acknowledgement a necessary event in trading with regard to the invention, and it can be omitted when the seller and/or buyer so wishes. The main purpose of the acknowledgement is to give a quick feedback to the buyer to indicate that the purchase event has proceeded in the intended manner. The actual delivery of the purchased goods to the buyer may take so long that the buyer may get nervous if he has no evidence of a successful purchase prior to the delivery.

The next example is the application of the invention to such a telecommunication event between a seller and a receiver, in which information, which should not become known by third parties, is transmitted several times. A situation like this is shown in Fig. 4. Such information may include information related to personal goods and services, such as ordering medicines or care services for various illnesses, or consulting a doctor via the data network. Let us consider, for example, going to a pharmacy via the Internet. In the first step, the buyer goes to the home page of the pharmacy, from which the buyer selects the required medicines by filling in a form in the Internet. The buyer can print the form, which contains confidential information, the names of the medicines in this example, and sends it by telefax in step 401 to the pharmacy. According to another embodiment, the buyer can forward

the form electrically to be transmitted by a telefax. If required, the encoding of the information can be arranged e.g. so that the buyer can download from the home page of the seller an encoding program to his personal computer and encode the confidential information before sending it to the seller. The seller's telefax and preferably also other data system receives the information sent by the buyer and transfers the information to the trade database. If the information is encoded, it is decoded, whereafter the information is transferred to the trade database. Preferably the trade system sends in step 402 acknowledgement to the buyer, in which acknowledgement it asks for the buyer's personal data and credit card data. This acknowledgement can be sent via an open data network, such as the Internet, because in this connection confidential information is not transmitted at all. The buyer receives the acknowledgement and fills in the required data, whereafter the buyer again transmits 403 the confidential information in a similar manner as above, i.e. via a closed telecommunication network to the seller. When desired and required, this confidential information can be encoded with the same encoding program, for example, as the information transmitted previously. The receiver, or in this exemplary embodiment the seller's telefax receives the transmitted information and transfers it to the data system. The seller's data system preferably combines the last received information with earlier information by means of a selected identifier, such as the telefax number. The seller can transmit 404 to the buyer verification of the reception of the confidential information, if the buyer and seller have so agreed. The verification can again be transmitted via the open data network.

It is clear to a person skilled in the art that the embodiments described above are exemplary and do not restrict the application of the invention in other ways than have been presented above. It has been assumed above that the purchasing process itself only takes place in one step, but it is clear that much more data transmission than has been presented above can take place before the confidential information is given. Confidential information can also be transmitted from the seller to the buyer e.g. when technical information related to the purchases, which the seller does not want to make known in the public, is transmitted. It is clear to a person skilled in the art that a modem, which is directly connected to the public switched telephone network, can also be used to transmit confidential information between the sender and receiver.

The solution according to the invention can also be used in cases in which the sender and receiver use other terminal devices than personal computers. As an example we may consider the case shown in Fig. 5, in which the sender or in this

exemplary embodiment the buyer uses a mobile station 501 to communicate with an open data network. In this exemplary embodiment, the mobile station is a mobile station 501 using the Global System for Mobile communications (GSM), which comprises means, by which it is possible to do business in the Internet. The mobile station 501 can also be e.g. a mobile station of a third generation mobile communication system, such as the UMTS (Universal Mobile Telecommunication System), or a mobile station 501 of any other telecommunication system, by which it is possible to establish a connection with an open data network, such as the Internet. In this exemplary embodiment, the user communicates with the Internet 108 by means of a mobile station 501. It is clear to a person skilled in the art that establishing a connection with the Internet 108 takes place so that there is a connection from the mobile station 501 to an open data network via a mobile communication network 502. Here the mobile communication network 502 is comparable to the public switched telephone network, or generally speaking represents a closed telecommunication network. The mobile communication network 502 comprises typical elements of a mobile communication network 502, such as base stations, base station controllers, mobile switching centres etc. It is clear to a person skilled in the art that the elements that belong to the mobile communication network 502 are dependent on the network being used, and the names and functions of the network elements can differ considerably between different networks. The user 501 of the mobile station selects the desired products from the Internet pages of a shop and sends his selection to the seller. The selection information or purchase information is transmitted partly via the mobile communication network 502 and partly via the Internet network 108. The seller's data system receives the transmission and transmits a form asking e.g. for the personal data and credit card data. The form can be transmitted to the buyer's mobile station 501 e.g. via the Internet 108 and the mobile communication network 502. Another possibility is that the seller transmits the form via the public switched telephone network 104 and the mobile communication network 502 to the mobile station 501. The form can be transmitted by using, for example, the Short Message Service (SMS) available in many telecommunication networks. Preferably the buyer transmits the required information by sending e.g. a short message to the seller. This naturally requires that the seller's data system can receive short messages. Another possibility is that the user of the mobile station 501 sends the required confidential information as a telefax to the seller's data system, in which the telefax is handled in a similar manner as in the embodiments presented above. It is known to a person skilled in the art that by a mobile station 501 a short message can be sent directly to the telefax device. This is possible at least in the GSM system. Complete telefax

services are being planned at least in the services of the future mobile communication networks. After the reception of confidential information, the seller can send to the user of the mobile station 501 acknowledgement of the reception of confidential information and e.g. the verification of the order. The arrangement described above does not include the possibility of encoding confidential information, but it is clear to a person skilled in the art that the encoding can also be arranged in the mobile station 501, if desired. For example, the seller can send an encoding program to the mobile station 501, which encoding program can be used by the user of the mobile station 401 to encode the confidential information.

It is clear to a person skilled in the art that although the embodiment according to the invention shown in Fig. 5 presents an arrangement in which the buyer uses a mobile station 501 and the seller a personal computer 107, it can also be implemented in other ways. For example, one possible arrangement is that the seller also uses a mobile station 501 instead of a personal computer, by means of which mobile station 501 the seller can request confidential information from the buyer. It is clear that the seller has arranged his home pages on a server in the open data network 108, whereby the buyer can get information about the products of the seller. Information about the products selected by the buyer is transmitted to the seller's mobile station 501. The transmission of confidential information is preferably implemented in such a case completely via the mobile communication network 502. It is also clear to a person skilled in the art that the mobile station 501 presented can be any other terminal, by which the operations mentioned above can be performed. The essential requirement is that in addition to the open data network, the terminal can also be connected to at least one other closed telecommunication network, which has better data security than an open data network.

It is clear to a person skilled in the art that the solutions presented above are only examples of the application of the invention and that the solution according to the invention can also be applied in other ways within the scope of the inventive idea defined by the attached claims. Although the application of the invention has above been described in connection with operations related to electric trade, it is clear that the invention can also be applied to all situations in which confidential information is to be transmitted.

Claims

1. A method for transmitting information between a sender and a receiver, at least part of which information is confidential information, **characterized** in that it comprises steps in which

- an encoding program is delivered to the sender via an open data network for processing confidential information,
- confidential information is processed with the encoding program, and
- the confidential information that have been processed with the encoding program are transmitted from the sender to the receiver via a closed telecommunication network.

2. A method according to Claim 1, **characterized** in that it also comprises a step in which the sender's connection setup is transmitted via an open telecommunication network to the receiver, whereby the step in which an encoding program is delivered to the sender via an open telecommunication network is performed as a response to the transmission of the sender's connection setup to the receiver.

3. A method according to Claim 1, **characterized** in that the step in which confidential information is processed with an encoding program includes a substep in which confidential information is encoded into an optically readable form.

4. A method according to Claim 3, **characterized** in that the confidential information is encoded into a bar code.

5. A method according to Claim 3, **characterized** in that the confidential information is encoded into an optically readable character string.

6. A method according to Claim 3, **characterized** in that the step in which the confidential information processed with an encoding program is transmitted from the sender to the receiver comprises a step in which the confidential information encoded into an optically readable form is transmitted in the form of a telefax via the telephone network.

7. A method according to Claim 6, **characterized** in that the step in which the confidential information processed with the encoding program is transmitted from the sender to the receiver includes steps in which

- the confidential information, which has been encoded to an optically readable form, is printed on paper, and

- a telefax representing said paper is transmitted to the receiver.

8. A method according to Claim 6, **characterized** in that the step in which the confidential information processed with an encoding program is transmitted from the sender to the receiver includes steps in which

- the confidential information, which has been encoded to an optically readable form, is converted to an electric bitmap form without printing it on paper, and

- the confidential information in the electric bitmap form is transmitted to the receiver.

9. A method according to Claim 1, **characterized** in that

- the step in which the confidential information is processed with an encoding program includes a substep, in which the confidential information is encoded to an acoustically readable form, and

- the step in which the confidential information processed with the encoding program are transmitted from the sender to the receiver includes a step in which the confidential information, which has been encoded to an acoustically readable form, is transmitted to the receiver as a tone frequency message via the telephone network.

10. A method according to Claim 1, **characterized** in that in the step, in which the confidential information is processed with an encoding program, the confidential information is also encrypted.

11. A method according to Claim 10, **characterized** in that in addition to the encoding program, the receiver's public key is delivered to the sender via the open telecommunication network, and the confidential information is encrypted with said public key.

12. A method according to Claim 1, **characterized** in that the sender can use the encoding program only once, and the sender's later use of the encoding program is prevented after the confidential information processed with the encoding program has been transmitted from the sender to the receiver.

13. A method according to Claim 1, **characterized** in that the encoding program is saved for later use, whereby the next transmission of confidential information from the sender to the receiver includes steps in which

- the confidential information is processed with the saved encoding program, and

- the confidential information processed with the encoding program are transmitted from the sender to the receiver via a closed telecommunication network.

14. A method according to Claim 1, **characterized** in that it also includes steps in which

- information is transmitted from the sender to the receiver also via an open telecommunication network, and

- the information, which has been transmitted to the receiver via the open telecommunication network, is combined with information, which has been transmitted to the receiver via a closed telecommunication network.

15. A method according to Claim 1, **characterized** in that it also includes steps in which

- the confidential information transmitted to the receiver is printed on paper,

- said information printed on paper is read optically into electric form, and

- the information, which has been read optically into electric form, is saved in the receiver's data system.

16. A method according to Claim 1, **characterized** in that it also includes steps in which

- the confidential information transmitted to the receiver is converted electrically from the form in which they were transmitted over the closed telecommunication network to another form without printing them on paper, and

- information, which has been electrically converted to another form, is saved in the receiver's data system.

17. A system for transmitting information between a sender and a receiver, at least part of which information is confidential, **characterized** in that it has

- means for delivering an encoding program via an open telecommunication network to the sender for processing confidential information,

- means for processing confidential information with an encoding program before delivering it from the sender to the receiver, and

- means for transmitting confidential information processed with an encoding program from the sender to the receiver via a closed telecommunication network.

18. A system according to Claim 17, **characterized** in that it also has means for combining the information transmitted via the open telecommunication network and the information transmitted via the closed telecommunication network to the receiver.

19. A system according to Claim 17, **characterized** in that the means for processing confidential information with an encoding program include means for producing a bar code.

20. A system according to Claim 17, **characterized** in that said open telecommunication network is the Internet.

21. A system according to Claim 17, **characterized** in that said closed telecommunication network is a public switched telephone network.

22. A system according to Claim 17, **characterized** in that said closed telecommunication network is a mobile communication network.

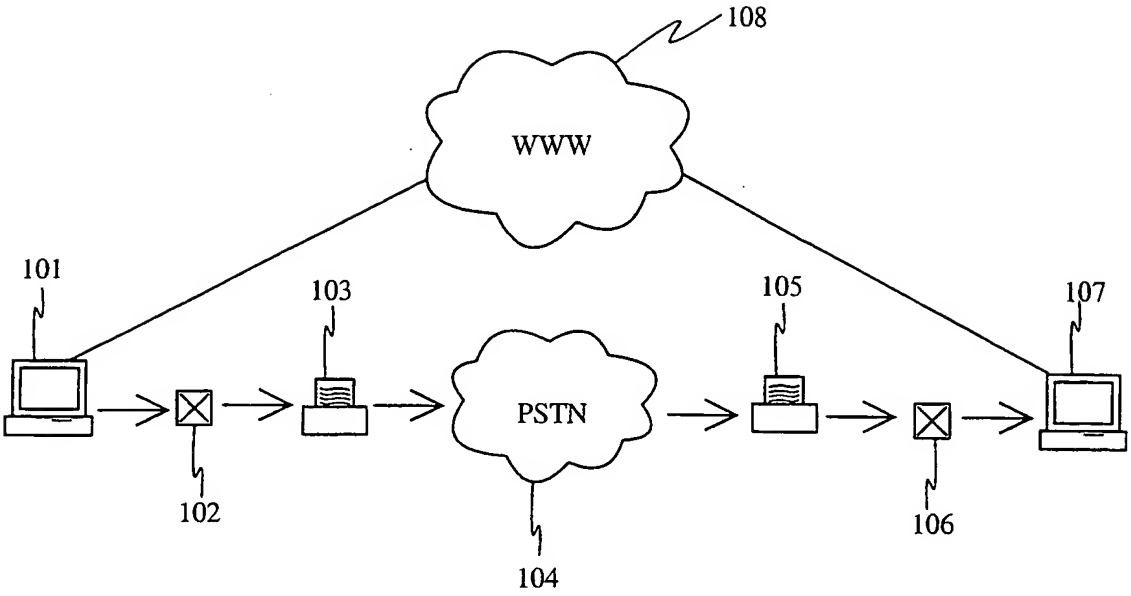

108
WWW
101
103
105
107
PSTN
102
104
106

Fig. 1

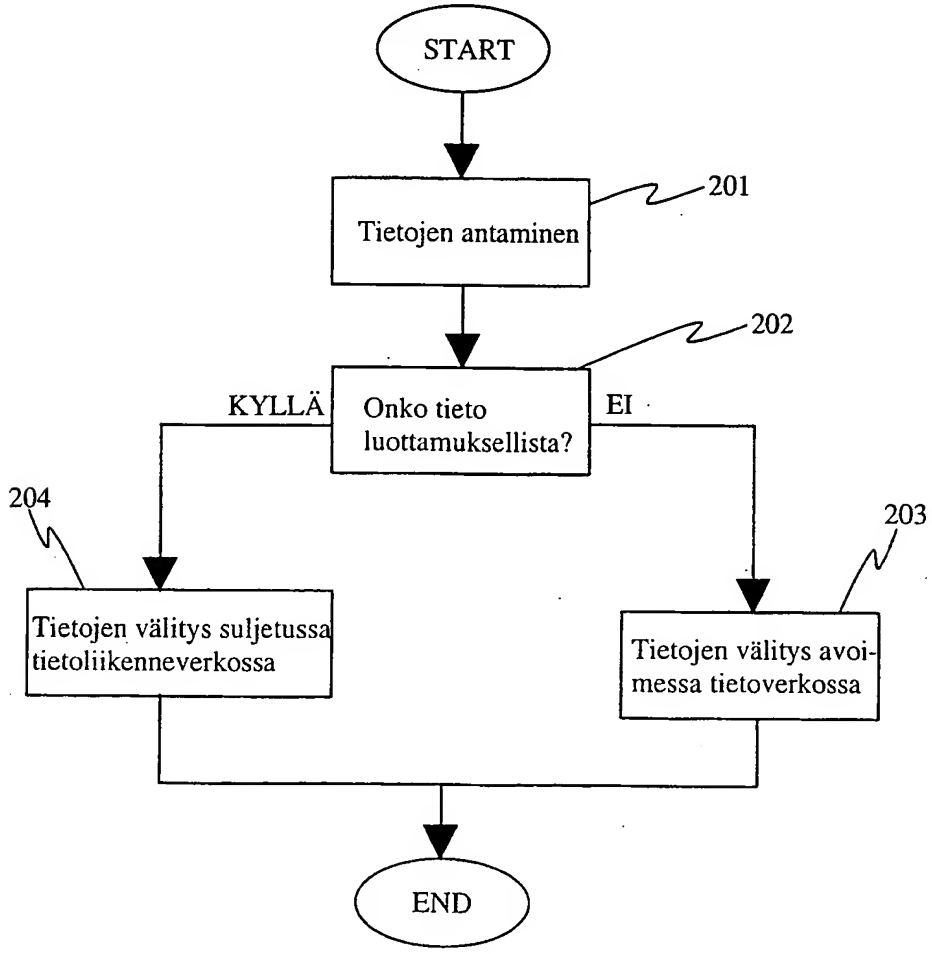

START
Tietojen antaminen
201
202
KYLLÄ
Onko tieto luottamuksellista?
EI
204
203
Tietojen välitys suljetussa tietoliikenneverkossa
Tietojen välitys avoimessa tietoverkossa
END

Fig. 2

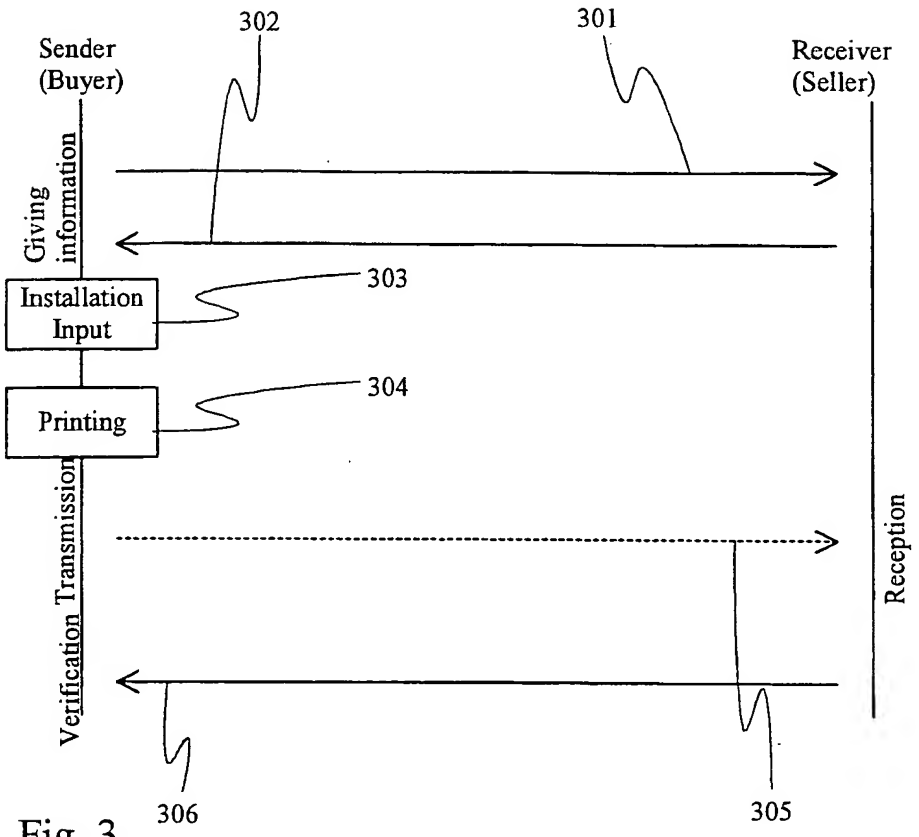

302
301
Sender
(Buyer)
Receiver
(Seller)
Giving information
303
Installation
Input
304
Printing
Verification Transmission
Reception
306
305

Fig. 3

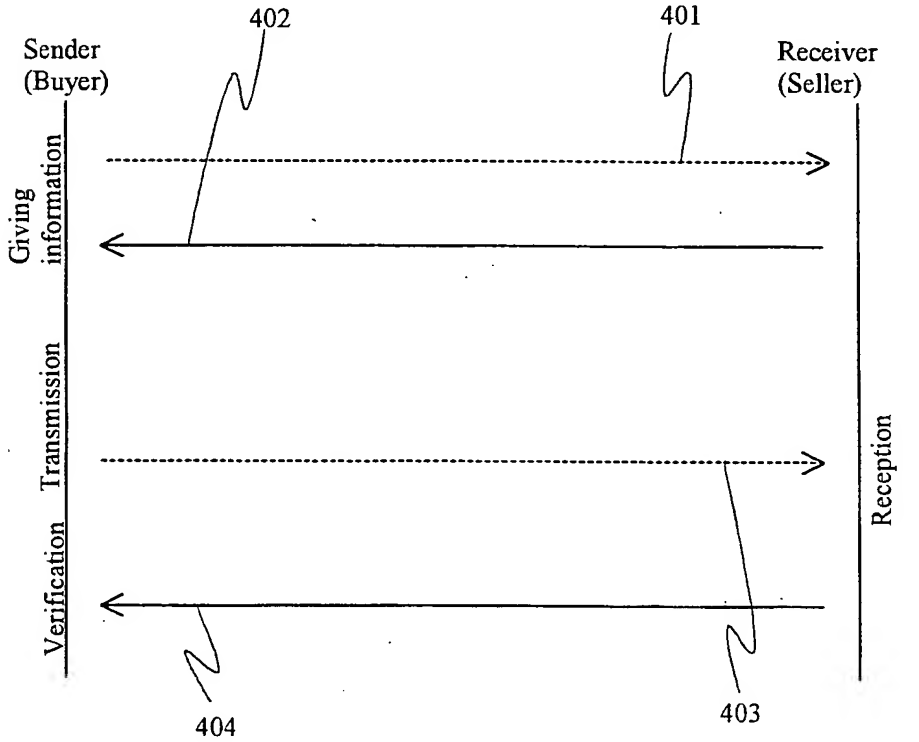

402
401
Sender
(Buyer)
Receiver
(Seller)
Giving information
Transmission
Verification
Reception
404
403

Fig. 4

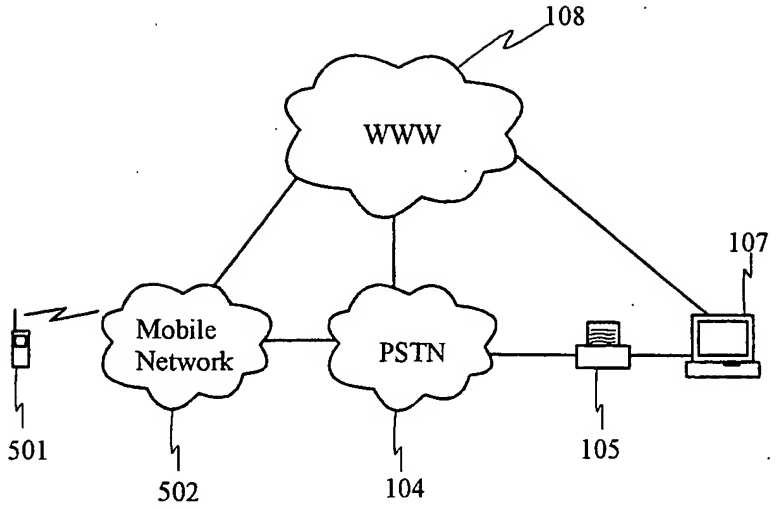


Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 00/00896

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 9/32
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0889620 A2 (OKI ELECTRIC INDUSTRY CO. LTD.), 7 January 1999 (07.01.99), column 11, line 42 - column 12, line 13, claims 1-2	1,2,10,11, 17,18,20,21, 22
A		12,13,14
	--	
A	EP 0765068 A2 (AT&T CORP.), 26 March 1997 (26.03.97), figure 1	1-22
	--	
A	WO 9934547 A1 (INTERACTIVE MAGAZINES LTD.), 8 July 1999 (08.07.99), abstract	1-22
	--	

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 February 2001	21 -02- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Rune Bengtsson/mj Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

27/12/00

International application No.
PCT/FI 00/00896

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0889620 A2	07/01/99	JP 11025046 A	29/01/99
EP 0765068 A2	26/03/97	AU 709790 B	09/09/99
		AU 6571896 A	27/03/97
		CA 2182818 A	23/03/97
		JP 9153964 A	10/06/97
		US 5745556 A	28/04/98
		US 5864610 A	26/01/99
WO 9934547 A1	08/07/99	AU 1775099 A	19/07/99
		GB 2332833 A	30/06/99
		GB 9727369 D	00/00/00